UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,481	07/23/2003	Makoto Fujiwara	60188-593	7409

7590 07/05/2007

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
NGUYEN, KHOI	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
07/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/624,481	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Khoi Nguyen	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/29/2005 and 04/03/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Claims 1, 8, and 10 have been amended and entered.

2. Claims 1-17 are pending and examined.

Response to Arguments

3. Applicant's arguments, see pages 11-13, filed 02/16/2007, with respect to the rejection(s) of claim(s) 1 and 17 under 35 USC 102(b) and 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Thurstom et al., in view of Giles et al., in view of Pavlin et al., in view of Asano et al. and further in view of of Feigenbaum et al.

4. Further considerations upon the new ground of rejections and in lieu of new references, examiner respectfully withdraw the allowable subject matter previously indicated in prior Office Action for claims 9, 11, and 15-16.

Claim Objections

5. Claim 12 is objected as lack of antecedent basic, "the step of installing" line 16.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 2 is rejected under 35 USC 112, second paragraph as being vague and indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention.

8. With regard to claim 2, the term "the LSI device" on lines 2 and 3 is not clearly understood as whether it is referring to the LSI device where the **final product** would be implemented or the LSI where the product is being **developed under different modes**. For the purpose of examining, "the LSI device" phase of the instant claim would be construe as the provided LSI where the product is being developed under different modes.

9. With regard to claim 2, the phase "when being set to the production operation mode, the LSI device cannot execute a raw (binary) program" on lines 3-4 of the instant claim is not clearly understood as how possible that an executable program would not run under a product operation mode. For the purpose of examining, examiner considers in the product operation mode only non-released version of the raw (binary) program cannot be run.

10. With regard to claim 2, the phase "raw (binary) program" on lines 3-4 of the instant claim is not clearly understood as it is referring to non compiled or linked

program ready to run under an OS. For the purpose of examining, the phase "raw (binary) program" hereafter will be construed as pre-compiled , pre-linked program ready to run under an OS.

Claim Rejections - 35 USC § 102

11. The following is a quotation of 35 U.S.C 102(e) which forms the basis for all rejections set forth in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claim 1 is rejected under 35 U.S.C 102(e) as anticipated by Thurston et al. (US PGPub No. 20030217193), hereafter "Thurston".

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

13. With regard to claim 1, Thurstom discloses a method for developing a program which is to be installed in a system having an LSI device (abstract), the method comprising the steps of:

Providing another LSI device having the same structure as that of the LSI device (Fig. 1: item 108a, since firmware update package must be developed on the same firmware of the updating entity; thus it reads on providing another LSI device having the same structure as the of the LSI device);

Setting the provided LSI device to a development mode so that the provided LSI device is used as a development LSI device, the development mode being different from a product operation mode employed at the times of program installation and product operation ([0056]: lines 1-11, firm ware update package and interactive installation mode reads on Setting the provided LSI device to a development mode so that the provided LSI device is used as a development LSI device, the development mode being different from a product operation mode employed at the times of program installation and product operation);

Developing the program on the development LSI device (Fig. 1: item 108a).

14. With regard to claim 2, Thurstom discloses the operation of the LSI device is restricted such that when being set to the development mode, the LSI device can

execute a raw (binary) program ([0065]: lines 4-5, vendor develops a binary firmware reads on the operation of the LSI device is restricted such that when being set to the development mode, the LSI device can execute a raw (binary) program), and when being set to the product operation mode, the LSI device cannot execute a raw (binary) program ([0047]: lines 7-8, updates firmware on hardware devices reads on when being set to the product operation mode, the LSI device cannot execute a raw (binary) program).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 3-4 are rejected under 35 USC 103(a) as unpatentable over Thurstom in view of Pavlin et al. (US PGPub 2001/0056539), hereafter " Pavlin".

17. With regard to claim 3, Thurstom discloses a program developed on the development LSI device at the program development step ([0065]: lines 4-5, vendor develops a binary firmware reads on a program developed on the development LSI device at the program development step). However Thurstom dose not disclose the step of encrypting the program.

Pavlin discloses the step of encrypting the program developed on the development LSI device at the program development step ([0032]: lines 24-26).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to include the step of encrypting the program, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

18. With regard to claim 4, Thurstom discloses the operation of the LSI device is restricted such that when being set to the development mode ([0065]: lines 4-5, vendor develops a binary firmware reads on the operation of the LSI device is restricted such that when being set to the development mode), the LSI device cannot generate a key for encrypting a raw (binary) program in the development mode).

However, Thurstom does not disclose the LSI device cannot generate a key for encrypting a raw (binary) program.

Pavlin, on the other hand, discloses the LSI device cannot generate a key for encrypting a raw (binary) program ([0040]: lines 8-10, packets are decrypted using CC1 decryption key stored in the hardware key reads on the operation of

the LSI device is restricted such that the LSI device cannot generate a key for encrypting a raw (binary) program).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that LSI device cannot generate a key for encrypting a raw (binary) program, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

19. With regard to claim 5, Thurstom discloses a method for developing a program which is to be installed in a system having an LSI device (abstract), further comprising the steps of:

Providing another LSI device having the same structure as that of the LSI device (Fig. 1: item 108a, since firmware update package must be developed on the same firmware of the updating entity; thus it reads on providing another LSI device having the same structure as the of the LSI device);

Setting the provided LSI to a mode ([0056]: lines 1-11, providing interactive mode during the installation of the firmware reads on setting the provided LSI to a mode)

Thurstom does not disclose a key-generation mode so that the provided LSI device is used as a key-generation LSI device, the key-generation mode being different from the development mode and the product operation mode, and installing an encrypted key-generation program in the key-generation LSI and executing the key-generation program to generate a key.

Pavlin, on the other hand, discloses setting the provided LSI device to a key-generation mode so that the provided LSI device is used as a key-generation LSI device ([0084]: lines 1-7, hardware key with the aid of developer key in combination to protect a software application reads on key-generation LSI device), the key-generation mode being different from the development mode and the product operation mode ([0085]: lines 5-6, encrypting partially a software application reads on key-generation mode being different from the development mode and the product operation mode), and installing an encrypted key-generation program in the key-generation LSI executing the key-generation program to generate a key ([0087]: lines 6-8, in order to encrypt, a key must be generated or provided to encrypt the string from a program or utility which reads on installing an encrypted key-generation program in the key-generation LSI executing the key-generation program to generate a key)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to set the

provided LSI device to a key-generation mode so that the provided LSI device is used as an key-generation LSI device, the key-generation mode being different from the development mode and the product operation mode, and executing the key-generation program to generate a key, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

20. With regard to claim 6, Thurstom discloses the operation of the LSI device is restricted such that when being set to a mode, the LSI device cannot execute a raw (binary) program ([0047]: updates firmware on the hardware device reads on operation of the LSI device is restricted such that when being set to a mode, the LSI device cannot execute a raw (binary) program).

However, Thurstom does not disclose the operation is being set to the key-generation mode, the LSI device cannot execute a raw (binary) program.

Pavlin, on the other hand discloses the operation of the LSI device is being set to the key-generation mode, the LSI device cannot execute a raw (binary) program ([0085]: lines 1-21).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that the operation is

being set to the key-generation mode, the LSI device cannot execute a raw (binary) program, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

21. With regard to claim 7, Thurstom discloses a method for developing a program which is to be installed in a system having an LSI device (abstract), further comprising the steps of:

Providing another LSI device having the same structure as that of the LSI device (Fig. 1: item 108a, since firmware update package must be developed on the same firmware of the updating entity; thus it reads on providing another LSI device having the same structure as the of the LSI device);

Setting the provided LSI to a mode ([0056]: lines 1-11, providing interactive mode during the installation of the firmware reads on setting the provided LSI to a mode).

Thurstom does not disclose setting the provided LSI device to an administrator mode so that the provided LSI device is used as an administrator LSI device, the administrator mode being different from the development mode, the product operation mode, and the key-generation mode; and developing the key-

generation program and encrypting the developed key-generation program with any key on the administrator LSI device.

Pavlin, on the other hand discloses setting the provided LSI device to an administrator mode so that the provided LSI device is used as an administrator LSI device ([0087]: lines 5-6, allowing compiler to encrypt the string reads on administrator mode), the administrator mode being different from the development mode, the product operation mode, and the key-generation mode ([0087]: operating in a compiler mode to encrypt a string reads on being different from development, product operation, and key-generation mode); and developing the key-generation program and encrypting the developed key-generation program with any key on the administrator LSI device ([0090]: lines 1-3, the hardware key contains encryption algorithm and key which was developed by the developer key reads on developing the key-generation program and encrypting the developed key-generation program with any key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to set the provided LSI device to an administrator mode so that the provided LSI device is used as an administrator LSI device, the administrator mode being different from the development mode, the product operation mode, and the key-generation mode; and developing the key-generation program and encrypting the developed

key-generation program with any key on the administrator LSI device, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

22. Claims 8-9, 12, 14-17 are rejected under 35 USC 103(a) as unpatentable over Thurstom, in view of Pavlin, and further in view of Asano et al. (US Pat. No. 7167564), hereafter "Asano".

23. With regard to claim 8, Thurstom discloses a program development support system (abstract), comprising:

A development LSI device having the same structure as that of an LSI device on which the program runs (Fig. 1: item 108a, since firmware update package must be developed on the same firmware of the updating entity; thus it reads on a development LSI device having the same structure as that of an LSI device on which the program runs); and

An external memory for storing a raw (binary) program (Fig. 1: item 108), wherein the development LSI device includes a memory for storing information, and the development LSI device is capable of executing a raw (binary) program ([0075]: lines 2-7, code or logic implemented in hardware logic in producing firmware for ASIC reads on the development LSI device includes a memory for storing

information, and the development LSI device is capable of executing a raw (binary) program)

input from the external memory (col. 6: lines 29-32; col. 24: lines 7-12, to be able to preview the result prior to the actual execution of the application from applications that stored in different devices on the network reads on capable of executing program input from the external memory)

However, Thurstom does not disclose a secure memory for storing common key information regarding a raw common key; a first step of obtaining the raw common key from the common key information stored in the secure memory, and a second step of encrypting using the raw common key.

Pavlin, on the other hand, discloses a secure memory for storing common key information regarding a raw common key (Fig. 2: item 114; [0044]: lines 4-8, CC1 algorithm and key reads on information regarding to a raw common key); a first step of obtaining the raw common key from the common key information stored in the secure memory ([0054]: lines 32-35, decryption of both message and program reads on first step of obtaining the raw common key from the common key information stored in the secure memory).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to provide a secure memory for storing common key information regarding a raw common key; a first step of obtaining the raw common key from the common key information stored in the secure memory, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

Nevertheless, neither Thurstom nor Pavlin discloses the second step of encrypting using the raw common key.

Asano, on the other hand, discloses the second step of encrypting using the raw common key (Fig. 8: item 81; col. 12: lines 51-57, Kcon is encrypted by K00 reads on encrypting the raw common key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom and Pavlin such that to include the step of encrypting using the raw common key, as taught by Asano, and would be motivated to provide a high degree of security and flexibility to provide the encrypted content key to an authorized user so that only the authorized user can decrypt the encrypted content key using a decryption key held only by the authorized user (Asano, col. 2: lines 47-50).

24. With regard to claims 9 and 15, Thurstom discloses the program development support system and method (abstract).

However, Thurstom does not disclose the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and the first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed.

Pavlin, on the other hand, discloses the key information ([0040]: lines 4-8).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to provide the key information, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

Nevertheless, neither Thurstom nor Pavlin discloses the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second

intermediate key; and the first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed.

Aseno, on the other hands, discloses the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key (Fig. 8: items 802 and 803, Kcon which is a common key encrypted by a raw key, KEK which is encrypted by another key, EKB reads on an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key); and

The first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed (Fig. 9, col. 15: lines 66-67, col. 16: lines 1-7; Fig. 8, the decryption process is well known in the art by performing the reversing procedure of the encryption process, thus, using the first intermediate key, KEK, to get to the common key, Kcon, and the EKB which construed as a program encryption seed since it was used as starting point for the encryption process to get to the first intermediate key. This reads on the step of obtaining the raw common key

using the encrypted common key, the encrypted first intermediate key and a program encryption seed).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom and Pavlin such that to include the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed, as taught by Asano, and would be motivated to provide a high degree of security and flexibility to provide the encrypted content key to an authorized user so that only the authorized user can decrypt the encrypted content key using a decryption key held only by the authorized user (Asano, col. 2: lines 47-50)..

25. With regard to claim 12, Thurstom discloses a method for installing a program in a system which includes an external memory and an LSI device (Abstract), the method comprising:

The initial procedure, first, second, third, fourth, and the step of installing the program in the LSI device (Fig. 6: items 600-610); a raw (binary) program in the LSI device, and a program supplied from the external memory (Fig. 1: item 108a firmware update package includes firmware update code and logics and being distributed to client 100 reads on a raw (binary) program in the LSI device, and a program supplied from the external memory).

However, Thurstom does not disclose a method for installing an encrypted program in a key-implemented system which includes a secure memory; an initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding a raw inherent key in the secure memory; the first step of obtaining the raw common key from the common key information store in the secure memory; a second step of decrypting a common key-encrypted program using the raw common key obtained at the first step; a third step of obtaining the raw inherent key from the inherent key information stored in the security memory; a fourth step of encrypting the program obtained at the second step using the raw inherent key obtained at the third step, thereby obtaining an inherent key-encrypted program; and the step of installing the inherent key-encrypted program obtained at the fourth step in the external memory.

Pavlin, on the other hand discloses a method for installing an encrypted program in a key-implemented system ([0013]: lines 6-11, Fig. 2: item 114) that includes a secure memory (Fig. 2: item 114); a first step of obtaining a key from the key information stored in the secure memory ([0040]: lines 8-10, keys used to decrypted the software segment are securely stored in the hardware key reads on obtaining a key from key information storing a key information in the security memory); a second step of decrypting a key-encrypted program into a raw (binary) program using the raw key obtained at the first step ([0054]: lines 32-35,

decrypt message and application using CC0 and CC1 stored in EEPROM, reads on decrypting a key-encrypted program using the raw key obtained in the first step)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to include a method for installing an encrypted program in a key-implemented system which includes a secure memory, the first step of obtaining the raw key from the key information store in the secure memory; a second step of decrypting a key-encrypted program using the raw key obtained at the first step, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

Nevertheless, neither Thurstom nor Pavlin discloses an initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding a raw inherent; obtaining the raw common key; decrypting using the raw common key; obtaining the raw inherent key from the inherent key information; encrypting using the raw inherent key; and the inherent key-encrypted data.

Aseno discloses an initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding

a raw inherent (Fig. 7: items EKB, "Data (encryption key" column, EKB contains common key information - K000 and K001, and inherent key information - K00, K0, and KR, reads on initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding a raw inherent key);

obtaining the raw common key from the common key information (col. 13: lines 27-29, device 2 can get common key K001 from EKB reads on obtaining the raw common key from the common key information).

decrypting using the raw common key (Fig. 9: item "Device 0"; col. 16: lines 1-6, getting Kcon using K(t)00 reads on decrypting using the raw common key);

obtaining the raw inherent key from the inherent key information (Fig. 7: item "Device 0" and K000; Fig. 9: items "Device 0" and "EKB"; col. 16: lines 1-3, getting K(t)00 using K000 since K000 is the child of K00; thus it is inherited any properties from its parent which stored in EKB information block reads on obtaining the raw inherent key from the inherent key information);

encrypting using the raw inherent key (Fig. 7B: item "Enc(K(t)001, K(t)00", since K(t)00 is the parent of K(t)001 and inherent the property by default in a tree

structure and encrypted by K(t)00; thus this reads on encrypting using the raw inherent key);

and the inherent key-encrypted data (Fig. 7: item "Enc(K0010, K(t)001)", Fig. 8B: items 805 and 804, each content or data were encrypted with a common key, Kcon and in turn encrypted by its inherent or parent key, KEK; thus resulting in the inherent key-encrypted data).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom and Pavlin such that to include an initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding a raw inherent; obtaining the raw common key; decrypting using the raw common key; obtaining the raw inherent key from the inherent key information; encrypting using the raw inherent key; and the inherent key-encrypted data, as taught by Asano, and would be motivated to provide a high degree of security and flexibility to provide the encrypted content key to an authorized user so that only the authorized user can decrypt the encrypted content key using a decryption key held only by the authorized user (Asano, col. 2: lines 47-50).

26. With regard to claim 14, Thurstom discloses information is stored in memory (Fig. 1: item 108a).

However, Thurstom does not disclose information store in an unrewritable area of the secure memory.

Pavlin, on the other hands discloses information store in an unrewritable area of the secure memory ([0070]: lines 5-6 and Fig. 2: item 114, uses the instruction in F/W ROM reads on information store in an unrewritable area of the secure memory)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom to include information store in an unrewritable area of the secure memory, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software (Pavlin, [0025: lines 1-2).

Nevertheless, neither Thurstom nor Pavlin discloses the inherent key information is stored.

Asano, discloses the inherent key information is stored (Fig. 7b, items "EKB", "Enc(K(t)001, K(t)00").

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom and Pavlin such that to

include the inherent key information is stored, as taught by Asano, and would be motivated to provide a high degree of security and flexibility to provide the encrypted content key to an authorized user so that only the authorized user can decrypt the encrypted content key using a decryption key held only by the authorized user (Asano, col. 2: lines 47-50).

27. With regard to claim 16 Thurstom discloses a method for installing a program in system which includes an external memory and an LSI device (Fig. 1: item 108a).

However, Thurstom does not disclose the key information includes an encrypted key which is obtained by encrypting the raw key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and the third step includes the step of obtaining the raw inherent key using the encrypted common key, the encrypted first intermediate key and an encryption seed.

Pavlin, on the other hand, discloses the key information ([0040]: lines 4-8).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to provide the

key information, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software ([0025: lines 1-2).

Nevertheless, neither Thurstom nor Pavlin discloses the inherent key information includes an encrypted inherent key which is obtained by encrypting the raw inherent key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and the third step includes the step of obtaining the raw inherent key using the encrypted inherent key, the encrypted first intermediate key and an encryption seed.

Aseno, on the other hands, discloses the inherent key information includes an encrypted inherent key which is obtained by encrypting the raw inherent key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key (Fig. 7: items EKB, Enc(K(t)001, K(t)00), Enc(K(t)00, K(t)0), EKB contains inherent key information. Enc(K(t)001, K(t)00) is the inherent encrypted key where K(t)00 is the first raw intermediate key used to encrypt the raw inherent key, and furthermore, K(t)00 was encrypted by K(t)0 which is a second intermediate key. This reads on the inherent key information includes an encrypted inherent key which is obtained by encrypting the raw inherent key with a raw first intermediate key and an encrypted first intermediate key which is

obtained by encrypting the raw first intermediate key with a second intermediate key); and the third step includes the step of obtaining the raw inherent key using the encrypted inherent key, the encrypted first intermediate key and an encryption seed (Fig. 7B; the decryption process is well known in the art by performing the reversing procedure of the encryption process, thus, decrypting the encrypted inherent key, Enc(K(t)001, K(t)00) using K(t)00 which is encrypted Enc(K(t)00, K(t)0), the first intermediate key to get to the raw inherent key, K(t)001, and since the EKB contains the root of the encryption tree. This reads on the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a encryption seed).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom and Pavlin such that to incorporate the inherent key information includes an encrypted inherent key which is obtained by encrypting the raw inherent key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and the third step includes the step of obtaining the raw inherent key using the encrypted inherent key, the encrypted first intermediate key and an encryption seed, as taught by Asano, and would be motivated to provide a high degree of security and flexibility to provide the encrypted content key to an authorized user so that only the

authorized user can decrypt the encrypted content key using a decryption key held only by the authorized user (Asano, col. 2: lines 47-50).

28. With regard to claim 17, neither Thurstom nor Asano discloses the inherent key information is an inherent ID which is inherent to the LSI.

Pavlin, discloses the inherent key information is an inherent ID which is inherent to the LSI ([0087]: lines 1-10, developer key which couples with developer computer reads on the inherent key information is an inherent ID which is inherent to the LSI.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Thurstom such that to provide an inherent ID which is inherent to the LSI, as taught by Pavlin, and would be motivated to provide a high degree of security and flexibility to protect software ([0025: lines 1-2).

29. Claims 10-11, 13 are rejected under 35 USC 103(a) as unpatentable in view of Thurstom, in view of Pavlin, in view of Asano, and further in view of Feigenbaum et al. (US Pat No. 5307497), hereafter "Feigenbaum".

30. With regard to claim 10, limitations for another LSI with the same structure on which the encrypted program runs, an external memory for storing a raw (binary) program where the development LSI includes a secure memory for storing common key information regarding to a raw common key, and the development LSI device executes a first step of obtaining a raw common key from the common key information stored in the secure memory and a second step of encrypting the raw (binary) program input from the external memory using the raw common key have already been discussed with combined teachings of Thurstom, Pavlin, and Asano above (see discussion of claim 8)

However, neither Thurstom, Pavlin, nor Asano discloses a boot ROM for storing a boot program and executing the boot program stored in the boot ROM

Feigenbaum discloses a boot ROM for storing a boot program and executing the boot program stored in the boot ROM (abstract).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom, Pavlin and Asano such that to include a boot ROM for storing a boot program and executing the boot program stored in the boot ROM, as taught by Feigenbaum, and would be motivated to take advantage of the speed at which ROM can be access in

several orders of magnitude faster than the speed at which a hard disk or a floppy diskette can be accessed (Feigenbaum, col. 1: lines 40-43).

31. With regard to claim 11, it is rejected for the reason as claim 9 above.

32. With regard to claim 13, Thurstom discloses the LSI for storing a program (col. 17: lines 28-30; col. 23: lines 38-40, storing development environment application reads on setting the provided LSI device to a development mode) and execute the program (col. 37: lines 31-33; col. 38: lines 55-59).

However, neither Thurstom, Pavlin, nor Asano discloses a boot ROM for storing a boot program and executing the boot program stored in the boot ROM, thereby executing the first to fourth steps.

Feigenbaum discloses a boot ROM for storing a boot program and executing the boot program stored in the boot ROM (abstract).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the methods of Thurstom, Pavlin and Asano such that to include a boot ROM for storing a boot program and executing the boot program stored in the boot ROM, as taught by Feigenbaum, and would be motivated to take advantage of the speed at which ROM can be access in

several orders of magnitude faster than the speed at which a hard disk or a floppy diskette can be accessed (Feigenbaum, col. 1: lines 40-43).

Conclusion

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US Pat. No. 5812671 to Ross, Jr. (Discloses an encryption method where the network gateway decrypts the message from a and encrypt the message again with recipient's secret key).

b. US Pat. No. 6226618 to Downs et al. (Discloses data encrypted by data decrypting key, data decrypting key being encrypted by first public key).

c. US RE39,166 to Gammie (Discloses a key first encypted with first secret serial number, the encrypted key is then encrypted with second serial no).

d. US Pat. No. 4864615 to Bennett et al (Discloses the reproduction of secure keys by distribution of generation data and encrypted prekey).

e. US Pat. No. 4218738 to Matyas et al (Discloses secure hardware for cryptographically generating and verification pattern of a potential computer user's identify number).

f. US Pat No. 5771287 to Gilley et al. (Discloses a programmable device with a unique serial number, correlating a secret key with each SN and relates the secret key with authorized features on the device).

g. US Pat. No. 6834111 to Nishimura et al. (Discloses an encrypted digital data obtained by encrypting digital data using a work key, and an encrypted work key; the work key is obtained by encrypted it with a control key).

h. US Pat. No. 7062718 to Kodosky et al. (Discloses a simulating environment to distributed update and configurations to different type of LSI).

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

35. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 6/21/07

Benjamin E. Lanier
Examiner AU 2132